KOMISJONI DELEGEERITUD MÄÄRUS (EL) 2022/1645,

14. juuli 2022,

millega kehtestatakse Euroopa Parlamendi ja nõukogu määruse (EL) 2018/1139 rakendamise eeskirjad nõuete osas, mis on seotud selliste infoturvariskide juhtimisega, mis võivad mõjutada komisjoni määrustega (EL) nr 748/2012 ja (EL) nr 139/2014 hõlmatud organisatsioonide lennuohutust, ning muudetakse komisjoni määrusi (EL) nr 748/2012 ja (EL) nr 139/2014

EUROOPA KOMISJON,

võttes arvesse Euroopa Liidu toimimise lepingut,

võttes arvesse Euroopa Parlamendi ja nõukogu 4. juuli 2018. aasta määrust (EL) 2018/1139, mis käsitleb tsiviillennunduse valdkonna ühisnorme ja millega luuakse Euroopa Liidu Lennundusohutusamet ning millega muudetakse Euroopa Parlamendi ja nõukogu määrusi (EÜ) nr 2111/2005, (EÜ) nr 1008/2008, (EL) nr 996/2010, (EL) nr 376/2014 ja Euroopa Parlamendi ja nõukogu direktiive 2014/30/EL ning 2014/53/EL ning tunnistatakse kehtetuks Euroopa Parlamendi ja nõukogu määrused (EÜ) nr 552/2004 ja (EÜ) nr 216/2008 ning nõukogu määrus (EMÜ) nr 3922/91, ([1]) eriti selle artikli 19 lõike 1 punkti g ja artikli 39 lõike 1 punkti b,

ning arvestades järgmist:

(1) Kooskõlas määruse (EL) 2018/1139 II lisa punkti 3.1 alapunktis b sätestatud oluliste nõuetega peavad projekteerimis- ja tootjaorganisatsioonid rakendama ohutusriskide juhtimise süsteemi ja hoidma seda töös.

(2) Lisaks peavad lennuväljade käitajad ja perrooniteenuste osutamise eest vastutavad organisatsioonid kooskõlas määruse (EL) 2018/1139 VII lisa punktides 2.2.1 ja 5.2 sätestatud oluliste nõuetega rakendama ohutusriskide juhtimise süsteemi ning seda töös hoidma.

(3) Põhjendustes 1 ja 2 osutatud ohutusriskid võivad tuleneda eri asjaoludest, sealhulgas projekteerimis- ja hooldusvigadest, inimtegevusega seotud aspektidest ning keskkonna- ja infoturvaohtudest. Seepärast tuleks põhjendustes 1 ja 2 osutatud organisatsioonide rakendatavate juhtimissüsteemide puhul lisaks juhuslikest sündmustest tulenevatele ohutusriskidele arvesse võtta ka infoturvaohtudest tulenevaid ohutusriske, kui kuritahtlike kavatsustega isikud võivad puudusi omakasupüüdlikult ära kasutada. Need infoturvariskid on tsiviillennundussektoris pidevalt suurenenud, kuna praegused infosüsteemid on omavahel üha tihedamalt seotud ja langevad üha sagedamini kuritahtlike rünnakute ohvriks.

(4) Nende infosüsteemidega seotud riskid ei piirdu küberruumi vastu suunatud võimalike rünnakutega, vaid hõlmavad ka ohte, mis võivad mõjutada protsesse ja menetlusi ning inimeste käitumist.

(5) Paljud organisatsioonid juba kasutavad digiteabe ja -andmete turvalisuse tagamiseks rahvusvahelisi standardeid, näiteks standardit ISO 27001. Need standardid ei pruugi täielikult hõlmata tsiviillennunduse kogu eripära.

(6) Seetõttu on asjakohane kehtestada nõuded selliste infoturvariskide juhtimiseks, mis võivad mõjutada lennuohutust.

(7) On oluline, et need nõuded hõlmaksid erinevaid lennundusvaldkondi ja nende liideseid, kuna lennundus koosneb omavahel tihedalt seotud süsteemidest. Seepärast tuleks neid kohaldada kõikide nende organisatsioonide suhtes, kellelt praegustele liidu lennuohutusalaste õigusaktide kohaselt juba nõutakse juhtimissüsteemi rakendamist.

(8) Käesolevas määruses sätestatud nõudeid tuleks järjepidevalt kohaldada kõigis lennundusvaldkondades viisil, mis mõjutaksid võimalikult vähe neid liidu lennuohutusalaseid õigusakte, mida asjaomaste valdkondade suhtes juba kohaldatakse.

([1]) ELT L 212, 22.8.2018, lk 1.

(9) Käesolevas määruses sätestatud nõuded ei tohiks mõjutada komisjoni rakendusmääruse (EL) 2015/1998 ([2]) lisa punktis 1.7 ega Euroopa Parlamendi ja nõukogu direktiivi (EL) 2016/1148 ([3]) artiklis 14 sätestatud infoturbe- ja küberturvalisusnõuete kohaldamist.

(10) Käesolevas õigusaktis kasutatud infoturbemääratluse tõlgendamisel ei tohiks see erineda direktiivis (EL) 2016/1148 sätestatud võrgu- ja infosüsteemide turvalisuse määratlusest.

(11) Selleks et vältida õiguslike nõuete dubleerimist, tuleks juhul, kui käesoleva määrusega hõlmatud organisatsioonide suhtes juba kohaldatakse põhjenduses 9 osutatud muudest liidu õigusaktidest tulenevaid julgestusnõudeid, mis on oma toimelt samaväärsed käesoleva määruse sätetega, pidada kõnealuste julgestusnõuete järgimist käesolevas määruses sätestatud nõuetele vastavaks.

(12) Käesoleva määrusega hõlmatud organisatsioonid, kelle suhtes juba kohaldatakse rakendusmäärusest (EL) 2015/1998 tulenevaid julgestusnõudeid, peaksid täitma ka käesoleva määruse I lisa (IS.D.OR.230 „Infoturbealane välisaruandluskava“) nõudeid, kuna rakendusmäärus (EL) 2015/1998 ei sisalda sätteid infoturvaintsidentidest asutusevälise teavitamise kohta.

(13) Komisjoni määrusi (EL) nr 748/2012 ([4]) ja (EL) nr 139/2014 ([5]) tuleks muuta, et luua seos eespool loetletud määrustega ette nähtud juhtimissüsteemide ja käesoleva määruse kohaste infoturbe halduse nõuete vahel.

(14) Selleks et anda organisatsioonidele piisavalt aega käesoleva määrusega kehtestatud uute eeskirjade ja menetluste järgimise tagamiseks, tuleks käesolevat määrust kohaldada kolme aasta möödumisel käesoleva määruse jõustumise kuupäevast.

(15) Käesolevas määruses sätestatud nõuded põhinevad arvamusel nr 03/2021, ([6]) mille amet on esitanud kooskõlas määruse (EL) 2018/1139 artikli 75 lõike 2 punktidega b ja c ning artikli 76 lõikega 1.

(16) Vastavalt määruse (EL) 2018/1139 artikli 128 lõikele 4 konsulteeris komisjon kooskõlas 13. aprilli 2016. aasta institutsioonidevahelises parema õigusloome kokkuleppes ([7]) sätestatud põhimõtetega iga liikmesriigi määratud ekspertidega,

ON VASTU VÕTNUD KÄESOLEVA MÄÄRUSE:

Artikkel 1

Reguleerimisese

Käesolevas määruses sätestatakse nõuded, mida artiklis 2 osutatud organisatsioonid peavad täitma, et avastada ja juhtida infoturvariske, mis võivad mõjutada lennuohutust ning tsiviillennunduses kasutatavaid info- ja kommunikatsioonitehnoloogia süsteeme ja andmeid, ning avastada infoturvasündmusi ja teha kindlaks infoturvaintsidentidena käsitatavad sündmused, mis võivad mõjutada lennuohutust, ning nendele infoturvaintsidentidele reageerida ja neist taastuda.

([2]) Komisjoni 5. novembri 2015. aasta rakendusmäärus (EL) 2015/1998, millega nähakse ette lennundusjulgestuse ühiste põhistandardite rakendamise üksikasjalikud meetmed (ELT L 299, 14.11.2015, lk 1).

([3]) Euroopa Parlamendi ja nõukogu 6. juuli 2016. aasta direktiiv (EL) 2016/1148 meetmete kohta, millega tagada võrgu- ja infosüsteemide turvalisuse ühtlaselt kõrge tase kogu liidus (ELT L 194, 19.7.2016, lk 1).

([4]) Komisjoni 3. augusti 2012. aasta määrus (EL) nr 748/2012, millega nähakse ette õhusõidukite ja nendega seotud toodete, osade ja seadmete lennukõlblikkuse ja keskkonnaohutuse sertifitseerimise ning projekteerimis- ja tootjaorganisatsioonide sertifitseerimise rakenduseeskirjad (ELT L 224, 21.8.2012, lk 1).

([5]) Komisjoni 12. veebruari 2014. aasta määrus (EL) nr 139/2014, millega kehtestatakse lennuväljadega seotud nõuded ja haldusmenetlused vastavalt Euroopa Parlamendi ja nõukogu määrusele (EÜ) nr 216/2008 (ELT L 44, 14.2.2014, lk 1).

([6]) https://www.easa.europa.eu/document-library/opinions

([7]) ELT L 123, 12.5.2016, lk 1.

Artikkel 2

Kohaldamisala

1. Käesolevat määrust kohaldatakse järgmiste organisatsioonide suhtes:

a) tootjaorganisatsioonid ja projekteerimisorganisatsioonid, kelle suhtes kohaldatakse määruse (EL) nr 748/2012 I lisa (osa 21) A jao G ja J alajagu, välja arvatud sellised projekteerimis- ja tootjaorganisatsioonid, kes tegelevad üksnes määruse (EL) nr 748/2012 artikli 1 lõike 2 punktis j määratletud ELA2 õhusõidukite projekteerimise ja/või tootmisega;

b) lennuväljade käitajad ja perrooniteenuste osutajad, kelle suhtes kohaldatakse määruse (EL) nr 139/2014 III lisa „Nõuded organisatsioonidele (osa ADR.OR)".

2. Käesolev määrus ei piira rakendusmääruse (EL) 2015/1998 lisa punktis 1.7 ega direktiivi (EL) 2016/1148 artiklis 14 sätestatud infoturbe- ja küberturvalisusnõuete kohaldamist.

Artikkel 3

Mõisted

Käesolevas määruses kasutatakse järgmisi mõisteid:

1) „infoturve" – võrgu- ja infosüsteemide konfidentsiaalsuse, tervikluse, autentsuse ja kättesaadavuse säilitamine;

2) „infoturvasündmus" – süsteemi, teenuse või võrgu puhul kindlaks tehtud ilming, mis osutab infoturvapoliitika võimalikule rikkumisele või infoturvakontrolli puudustele või seni tundmatule olukorrale, mis võib olla infoturbe seisukohast oluline;

3) „intsident" – sündmus, mis kahjustab direktiivi (EL) 2016/1148 artikli 4 punktis 7 määratletud võrgu- ja infosüsteemide turvalisust;

4) „infoturvarisk" – infoturvasündmuse toimumise võimalusest tulenev risk organisatsiooni tsiviillennundustegevusele, varale, isikutele ja teistele organisatsioonidele. Infoturvariskid on seotud võimalusega, et potentsiaalsed ohuallikad kasutavad ära teabevara või teabevarade rühma turvaauke;

5) „ohuallikas" – võimalik infoturbealane rikkumine, mis esineb kahju põhjustada võiva üksuse olemasolu või asjaolu, tegevuse või sündmuse esinemise korral;

6) „turvaauk" – vara või süsteemi, menetluse, projekti, rakendamise või infoturvameetmete viga või puudus, mida saab ära kasutada ja mille tulemuseks on vastuolu infoturvapoliitika nõuetega või nende rikkumine.

Artikkel 4

Muudest liidu õigusaktidest tulenevad nõuded

1. Kui artiklis 2 osutatud organisatsioon vastab direktiivi (EL) 2016/1148 artiklis 14 sätestatud turvanõuetele, mis on samaväärsed käesolevas määruses sätestatud nõuetega, loetakse nende turvanõuete täitmine käesolevas määruses sätestatud nõuetele vastavaks.

2. Kui artiklis 2 osutatud organisatsioon on käitaja või üksus, millele on osutatud liikmesriikide riiklikes tsiviillennundusjulgestuse programmides, mis on kehtestatud kooskõlas Euroopa Parlamendi ja nõukogu määruse (EÜ) nr 300/2008 ([8]) artikliga 10, loetakse rakendusmääruse (EL) 2015/1998 lisa punktis 1.7 esitatud küberturvalisusnõuded samaväärseks käesolevas määruses sätestatud nõuetega, välja arvatud käesoleva määruse lisa punkt IS.D.OR.230, mille nõuded peavad olema täidetud.

([8]) Euroopa Parlamendi ja nõukogu 11. märtsi 2008. aasta määrus (EÜ) nr 300/2008, mis käsitleb tsiviillennundusjulgestuse ühiseeskirju ja millega tunnistatakse kehtetuks määrus (EÜ) nr 2320/2002 (ELT L 97, 9.4.2008, lk 72).

3. Komisjon võib pärast EASA ja direktiivi (EL) 2016/1148 artiklis 11 osutatud koostöörühmaga konsulteerimist anda välja suunised käesolevas määruses ja direktiivis (EL) 2016/1148 sätestatud nõuete samaväärsuse hindamiseks.

Artikkel 5

Pädev asutus

1. Asutus, kes vastutab käesolevas määruses sertifitseerimise ja järelevalve suhtes kehtestatud nõuete täitmise eest, on järgmine:

a) artikli 2 punktis a osutatud organisatsioonide puhul määruse (EL) nr 748/2012 I lisa (osa 21) kohaselt määratud pädev asutus;

b) artikli 2 punktis b osutatud organisatsioonide puhul määruse (EL) nr 139/2014 III lisa (ADR.OR-osa) kohaselt määratud pädev asutus;

2. Liikmesriigid võivad käesoleva määruse kohaldamisel määrata sõltumatu ja eraldiseisva üksuse, kes täidab lõikes 1 osutatud pädevate asutuste ülesandeid ja kohustusi. Sel juhul lepitakse kõnealuse üksuse ja lõikes 1 osutatud pädevate asutuste vahel kokku koordineerimismeetmed, et tagada tõhus järelevalve kõigi nõuete üle, mida asjaomane organisatsioon peab täitma.

Artikkel 6

Määruse (EL) nr 748/2012 muutmine

Määruse (EL) nr 748/2012 I lisa (osa 21) muudetakse järgmiselt:

1) sisukorda muudetakse järgmiselt.

   a) pealkirja 21.A.139 järele lisatakse järgmine pealkiri:

      „**21.A.139A Infoturbe halduse süsteem**“;

   b) pealkirja 21.A.239 järele lisatakse järgmine pealkiri:

      „**21.A.239A Infoturbe halduse süsteem**“;

2) punkti 21.A.139 järele lisatakse punkt 21.A.139A:

   „**21.A.139A Infoturbe halduse süsteem**

   Lisaks punktis 21.A.139 nõutud tootmisjuhtimissüsteemile kehtestab tootjaorganisatsioon kooskõlas komisjoni delegeeritud määrusega (EL) 2022/1645 (*) infoturbe halduse süsteemi, et tagada selliste infoturvariskide nõuetekohane juhtimine, mis võivad mõjutada lennuohutust, ning rakendab süsteemi ja hoiab seda töös.

   (*) Komisjoni 14. juuli 2022. aasta delegeeritud määrus (EL) 2022/1645, millega kehtestatakse Euroopa Parlamendi ja nõukogu määruse (EL) 2018/1139 rakendamise eeskirjad nõuete osas, mis on seotud selliste infoturvariskide juhtimisega, mis võivad mõjutada komisjoni määrustega (EL) nr 748/2012 ja (EL) nr 139/2014 hõlmatud organisatsioonide lennuohutust, ning muudetakse komisjoni määrusi (EL) nr 748/2012 ja (EL) nr 139/2014 (ELT L 248, 26.9.2022, lk 18).“;

3) punkti 21.A.239 järele lisatakse punkt 21.A.239A:

   „**21.A.239A Infoturbe halduse süsteem**

   Lisaks punktis 21.A.239 nõutavale projekteerimise juhtimissüsteemile kehtestab projekteerimisorganisatsioon kooskõlas delegeeritud määrusega (EL) 2022/1645 infoturbe halduse süsteemi, et tagada selliste infoturvariskide nõuetekohane juhtimine, mis võivad mõjutada lennuohutust, ning rakendab süsteemi ja hoiab seda töös.“

Artikkel 7

Määruse (EL) nr 139/2014 muutmine

Määruse (EL) nr 139/2014 III lisa (ADR.OR-osa) muudetakse järgmiselt:

1) punkti ADR.OR.D.005 järele lisatakse punkt ADR.OR.D.005A:

„**ADR.OR.D.005A Infoturbe halduse süsteem**

Lennuvälja käitaja kehtestab kooskõlas komisjoni delegeeritud määrusega (EL) 2022/1645 (*) infoturbe halduse süsteemi, et tagada selliste infoturvariskide nõuetekohane juhtimine, mis võivad mõjutada lennuohutust, ning rakendab süsteemi ja hoiab seda töös.

(*) Komisjoni 14. juuli 2022. aasta delegeeritud määrus (EL) 2022/1645, millega kehtestatakse Euroopa Parlamendi ja nõukogu määruse (EL) 2018/1139 rakendamise eeskirjad nõuete osas, mis on seotud selliste infoturvariskide juhtimisega, mis võivad mõjutada komisjoni määrustega (EL) nr 748/2012 ja (EL) nr 139/2014 hõlmatud organisatsioonide lennuohutust, ning muudetakse komisjoni määrusi (EL) nr 748/2012 ja (EL) nr 139/2014 (ELT L 248, 26.9.2022, lk 18).“;

2) punkt ADR.OR.D.007 asendatakse järgmisega:

„**ADR.OR.D.007 Aeronavigatsiooniandmete ja -teabe haldamine**

a) Lennuvälja käitaja rakendab ja haldab oma juhtimissüsteemi osana kvaliteedijuhtimissüsteemi, mis hõlmab järgmist:

1) aeronavigatsiooniandmetega seonduv tegevus;

2) aeronavigatsiooniteabe pakkumine.

b) Lennuvälja käitaja kehtestab oma juhtimissüsteemi osana ohutusjuhtimissüsteemi, et tagada talle edastatud, tema kogutud või muul viisil kasutatavate operatiivandmete turvalisus, tehes need operatiivandmed kättesaadavaks üksnes volitatud isikutele.

c) Ohutusjuhtimissüsteemis määratakse kindlaks järgmised elemendid:

1) menetlused, mis on seotud andmeriski hindamise ja leevendamisega, julgestuse jälgimise ja parandamisega, julgestuse ümberhindamise ja kogemuste levitamisega;

2) vahendid, mis on kavandatud julgestusega seotud puuduste avastamiseks ja töötajate teavitamiseks asjakohastest hoiatustest;

3) vahendid julgestusega seotud puuduste kontrollimiseks ning parandusmeetmete ja leevendusmenetluste kindlaksmääramiseks, et vältida puuduste taastekkimist.

d) Lennuvälja käitaja tagab aeronavigatsiooniandmetega seoses oma töötajate julgeolekukontrolli.

e) Infoturbeaspekte hallatakse vastavalt punktile ADR.OR.D.005A.“;

3) punkti ADR.OR.F.045 järele lisatakse punkt ADR.OR.F.045A:

„**ADR.OR.F.045A Infoturbe halduse süsteem**

Perrooniteenuste osutamise eest vastutav organisatsioon kehtestab kooskõlas delegeeritud määrusega (EL) 2022/1645 infoturbe halduse süsteemi, et tagada selliste infoturvariskide nõuetekohane juhtimine, mis võivad mõjutada lennuohutust, ning rakendab süsteemi ja hoiab seda töös.“

Artikkel 8

Käesolev määrus jõustub kahekümnendal päeval pärast selle avaldamist *Euroopa Liidu Teatajas*.

Seda kohaldatakse alates 16. oktoobrist 2025.

Käesolev määrus on tervikuna siduv ja vahetult kohaldatav kõikides liikmesriikides.

Brüssel, 14. juuli 2022

Komisjoni nimel
president
Ursula VON DER LEYEN

LISA

INFOTURVE – ORGANISATSIOONIDELE ESITATAVAD NÕUDED

[IS.D.OR-OSA]

IS.D.OR.100 Kohaldamisala

Käesoleva osaga kehtestatakse nõuded, mida käesoleva määruse artiklis 2 osutatud organisatsioonid peavad täitma.

IS.D.OR.200 Infoturbe halduse süsteem

a) Organisatsioon kehtestab artiklis 1 sätestatud eesmärkide täitmiseks infoturbe halduse süsteemi ning rakendab ja hoiab seda töös, tagamaks, et organisatsioon:

   1) kehtestab infoturvapoliitika, milles sätestatakse organisatsiooni üldpõhimõtted seoses infoturberiskide võimaliku mõjuga lennuohutusele;

   2) teeb kindlaks ja vaatab läbi infoturvariskid kooskõlas punktiga IS.D.OR.205;

   3) määrab kindlaks infoturvariski käsitlemise meetmed ja rakendab neid kooskõlas punktiga IS.D.OR.210;

   4) rakendab infoturbealast sisearuandluskava kooskõlas punktiga IS.D.OR.215;

   5) kooskõlas punktiga IS.D.OR.220 määrab kindlaks meetmed, mida on vaja infoturvasündmuste avastamiseks, ja rakendab neid meetmeid, teeb kindlaks juhtumid, mida käsitatakse intsidentidena, mis võivad mõjutada lennuohutust, välja arvatud punkti IS.D.OR.205 alapunkti e kohaselt lubatud juhud, ning reageerib nendele infoturvaintsidentidele ja võtab meetmeid neist taastumiseks;

   6) rakendab meetmeid, millest pädev asutus on teatanud kui viivitamatust reageeringust lennuohutust mõjutavale infoturvaintsidendile või turvaaugule;

   7) võtab kooskõlas punktiga IS.D.OR.225 asjakohaseid meetmeid pädeva asutuse teatatud puuduste kõrvaldamiseks;

   8) rakendab punkti IS.D.OR.230 kohast välisaruandluskava, et pädev asutus saaks võtta asjakohaseid meetmeid;

   9) järgib punkti IS.D.OR.235 nõudeid, kui sõlmib punktis IS.D.OR.200 osutatud tegevuse mis tahes osa kohta allhankelepingu mõne muu organisatsiooniga;

10) järgib punkti IS.D.OR.240 kohaseid nõudeid töötajatele;

11) järgib punkti IS.D.OR.245 kohaseid andmesäilitusnõudeid;

12) jälgib organisatsiooni vastavust käesoleva määruse nõuetele ja annab puuduste kohta tagasisidet vastutavale juhatajale või projekteerimisorganisatsioonide puhul projekteerimisorganisatsiooni juhile, et tagada parandusmeetmete tõhus rakendamine;

13) kaitseb kogu sellise teabe konfidentsiaalsust, mida organisatsioon võib olla saanud teistelt organisatsioonidelt, vastavalt teabe tundlikkustasemele, ilma et see piiraks intsidentidest teatamise suhtes kohaldatavate nõuete järgimist.

b) Artiklis 1 osutatud nõuete pidevaks täitmiseks peab organisatsioon rakendama pidevat täiustamisprotsessi kooskõlas punktiga IS.D.OR.260.

c) Organisatsioon dokumenteerib kooskõlas punktiga IS.D.OR.250 kõik olulised protsessid, menetlused, rollid ja kohustused, mida on vaja punkti IS.D.OR.200 alapunkti a järgimiseks, ning kehtestab korra asjaomaste dokumentide muutmiseks. Kõnealuste protsesside, menetluste, rollide ja kohustustega seotud muudatusi hallatakse kooskõlas punktiga IS.D.OR.255.

d) Organisatsiooni poolt punkti IS.D.OR.200 alapunkti a täitmiseks kehtestatud protsessid, menetlused, rollid ja kohustused peavad vastama organisatsiooni tegevuse laadile ja keerukusele, lähtudes selle tegevusega kaasnevate infoturvariskide hindamisest, ning need võib integreerida muudesse olemasolevatesse juhtimissüsteemidesse, mida organisatsioon juba rakendab.

e) Ilma et see piiraks kohustust täita Euroopa Parlamendi ja nõukogu määruses (EL) nr 376/2014 ([1]) sätestatud aruandlusnõudeid ja punkti IS.D.OR.200 alapunkti a alapunktis 13 sätestatud nõudeid, võib pädev asutus anda organisatsioonile loa mitte rakendada alapunktides a–d osutatud nõudeid ja punktides IS.D.OR.205–IS.D.OR.260 sisalduvaid asjaomaseid nõudeid, kui organisatsioon tõendab kõnealust pädevat asutust rahuldaval viisil, et toimingud, mida ta teostab, rajatised, mida ta pakub, ressursid, mis talle eraldatakse ja teenused, mida ta osutab, ei põhjusta ei talle endale ega teistele organisatsioonidele infoturvariske, mis võivad mõjutada lennuohutust. See luba põhineb infoturvariskide dokumenteeritud hindamisel, mille teostab organisatsioon või kolmas isik kooskõlas punktiga IS.D.OR.205 ning mille on läbi vaadanud ja heaks kiitnud pädev asutus.

Pädev asutus vaatab kõnealuse loa kehtivuse üle pärast kohaldatavat järelevalveauditi tsüklit ja iga kord, kui organisatsiooni tööde maht muutub.

IS.D.OR.205 Infoturbe halduse süsteem

a) Organisatsioon teeb kindlaks kõik oma elemendid, mida võivad ähvardada infoturvariskid. Need hõlmavad järgmist:

1) toimingud, mida organisatsioon teostab, rajatised, mida ta pakub, ressursid, mis talle eraldatakse ja teenused, mida ta osutab;

2) seadmed, süsteemid, andmed ja teave, mis aitavad kaasa alapunktis 1 loetletud elementide toimimisele.

b) Organisatsioon teeb kindlaks liidesed, mis tal on teiste organisatsioonidega ja mis võivad vastastikku põhjustada infoturvariske.

c) Alapunktides a ja b osutatud elementide ja liideste puhul teeb organisatsioon kindlaks infoturvariskid, mis võivad mõjutada lennuohutust. Organisatsioon teeb iga kindlakstehtud riski puhul järgmist:

1) määrab riskitaseme vastavalt organisatsiooni kehtestatud ja eelnevalt kindlaks määratud liigitusele;

([1]) Euroopa Parlamendi ja nõukogu 3. aprilli 2014. aasta määrus (EL) nr 376/2014, mis käsitleb tsiviillennunduses toimunud juhtumitest teatamist ning juhtumite analüüsi ja järelmeid, millega muudetakse Euroopa Parlamendi ja nõukogu määrust (EL) nr 996/2010 ning tunnistatakse kehtetuks Euroopa Parlamendi ja nõukogu direktiiv 2003/42/EÜ ja komisjoni määrused (EÜ) nr 1321/2007 ja (EÜ) nr 1330/2007 (ELT L 122, 24.4.2014, lk 18).

2) seostab iga riski ja selle taseme alapunktide a ja b kohaselt kindlaks määratud asjakohase elemendi või liidesega.

Alapunktis 1 osutatud eelnevalt kindlaksmääratud liigituse puhul võetakse arvesse ohustsenaariumi esinemise võimalust ja selle ohutusalaste tagajärgede raskusastet. Sellele liigitusele tuginedes ja võttes arvesse, kas organisatsioonil on toimingute jaoks struktureeritud ning korratav riskijuhtimisprotsess, peab organisatsioon suutma kindlaks teha, kas risk on vastuvõetav või tuleb seda käsitleda kooskõlas punktiga IS.D.OR.210.

Selleks et riskihindamisi oleks vastastikku hõlpsam võrrelda, võetakse alapunkti 1 kohasel riskitaseme määramisel arvesse asjakohast teavet, mis on kogutud koostöös alapunktis b osutatud organisatsioonidega.

d) Organisatsioon vaatab alapunktide a, b ja c kohaselt tehtud riskihindamise läbi ja ajakohastab seda kõikidel järgmistel juhtudel:

1) infoturvariskiga seotud elemendid on muutunud;

2) organisatsiooni ja teiste organisatsioonide vahelised liidesed või teiste organisatsioonide teatatud riskid on muutunud;

3) riskide kindlakstegemiseks, analüüsimiseks ja liigitamiseks kasutatud teave või teadmised on muutunud;

4) infoturvaintsidente analüüsides on saadud uusi teadmisi.

IS.D.OR.210 Infoturvariski käsitlemine

a) Organisatsioon töötab välja meetmed punkti IS.D.OR.205 kohaselt kindlaks tehtud vastuvõetamatute riskide käsitlemiseks, rakendab neid õigel ajal ja kontrollib nende jätkuvat tõhusust. Need meetmed võimaldavad organisatsioonil teha järgmist:

1) kontrollida asjaolusid, mis aitavad kaasa ohustsenaariumi tõhusale esinemisele;

2) vähendada ohustsenaariumi realiseerumisest tulenevaid tagajärgi lennuohutusele;

3) vältida riske.

Kõnealuste meetmetega ei kaasne uusi võimalikke vastuvõetamatuid riske lennuohutusele.

b) Punkti IS.D.OR.240 alapunktides a ja b osutatud isikut ja organisatsiooni teisi mõjutatud töötajaid teavitatakse punkti IS.D.OR.205 kohaselt tehtud riskihindamise tulemustest, asjaomastest ohustsenaariumidest ja rakendatavatest meetmetest.

Organisatsioon teavitab ka selliseid organisatsioone, kellega tal on punkti IS.D.OR.205 alapunkti b kohane liides, mis tahes riskidest, mida kumbki organisatsioon teisega jagab.

IS.D.OR.215 Infoturbealane sisearuandluskava

a) Organisatsioon kehtestab asutusesisese aruandluskava, mis võimaldab talletada ja hinnata infoturvasündmusi, sealhulgas neid, millest tuleb teatada vastavalt punktile IS.D.OR.230.

b) Kõnealune kava ja punktis IS.D.OR.220 osutatud protsess peavad võimaldama organisatsioonil teha järgmist:

1) välja selgitada, milliseid alapunkti a kohaselt teatatud juhtumeid peetakse infoturvaintsidentideks või turvaaukudeks, mis võivad mõjutada lennuohutust;

2) teha kindlaks alapunkti 1 kohaselt avastatud infoturvaintsidentide ja turvaaukude põhjused ning neid mõjutavad tegurid ning käsitleda neid infoturvariskide juhtimise protsessi osana kooskõlas punktidega IS.D.OR.205 ja IS.D.OR.220;

3) tagada, et hinnatakse kogu teadaolevat asjakohast teavet, mis on seotud alapunkti 1 kohaselt kindlaks tehtud infoturvaintsidentide ja turvaaukudega;

4) vajaduse korral tagada, et rakendatakse meetodit teabe asutusesiseseks levitamiseks.

c) Kõik allhankelepingu alusel tegutsevad organisatsioonid, kes põhjustavad asjaomasele organisatsioonile infoturvariske, mis võivad mõjutada lennuohutust, peavad teavitama organisatsiooni infoturvasündmustest. Kõnealune teave esitatakse konkreetsetes allhankelepingutes kehtestatud korras ja seda hinnatakse vastavalt alapunktile b.

d) Organisatsioon teeb uurimise käigus koostööd kõigi teiste organisatsioonidega, kes on märkimisväärselt panustanud oma tegevusega seotud infoturbesse.

e) Organisatsioon võib selle aruandlussüsteemi integreerida muude aruandlussüsteemidega, mida ta on juba rakendanud.

IS.D.OR.220 Infoturvaintsidendid – nende avastamine, neile reageerimine ja nendest taastumine

a) Organisatsioon rakendab punkti IS.D.OR.205 kohaselt tehtud riskihindamise tulemuste ja punkti IS.D.OR.210 kohaselt tehtud riskikäsitluse tulemuste põhjal meetmeid, et teha kindlaks sellised intsidendid ja turvaaugud, mille puhul võivad realiseeruda vastuvõetamatud riskid ja mis võivad mõjutada lennuohutust. Kõnealused avastamismeetmed võimaldavad organisatsioonil teha järgmist:

1) avastada kõrvalekalded eelnevalt kindlaks määratud funktsionaalse tulemuslikkuse lähtetasemetest;

2) anda hoiatus, et kõrvalekalde korral aktiveerida nõuetekohased reageerimismeetmed.

b) Organisatsioon rakendab meetmeid, et reageerida alapunkti a kohaselt kindlaks tehtud sündmusele, mis võib muutuda või olla muutunud infoturvaintsidendiks. Kõnealused reageerimismeetmed võimaldavad organisatsioonil teha järgmist:

1) reageerida alapunkti a alapunktis 2 osutatud hoiatustele, aktiveerides eelnevalt kindlaks määratud vahendid ja tegevussuunad;

2) piirata rünnaku levikut ja vältida ohustsenaariumi täielikku realiseerumist;

3) kontrollida punkti IS.D.OR.205 alapunktis a kindlaks määratud asjaomaste elementide tõrkeolekut.

c) Organisatsioon rakendab infoturvaintsidentidest taastumiseks meetmeid, sealhulgas vajaduse korral erakorralisi meetmeid. Kõnealused taastumismeetmed võimaldavad organisatsioonil:

1) kõrvaldada intsidendi põhjustanud olukorra või muuta intsidendi ohutase vastuvõetavaks;

2) saavutada punkti IS.D.OR.205 alapunktis a kindlaks määratud asjaomaste elementide ohutus ajavahemiku jooksul, mille organisatsioon on taastumiseks eelnevalt kindlaks määranud.

IS.D.OR.225 Reageerimine pädeva asutuse teatatud puudustele

a) Kui pädevalt asutuselt saadakse teade puuduse kohta, teeb organisatsioon järgmist:

1) selgitab välja nõuetele mittevastavuse algpõhjuse või -põhjused ja nõuetele mittevastavust soodustavad tegurid;

2) töötab välja parandusmeetmete kava;

3) tõendab pädevat asutust rahuldaval viisil, et nõuetele mittevastavus on kõrvaldatud.

b) Alapunktis a osutatud meetmed võetakse pädeva asutusega kokkulepitud aja jooksul.

IS.D.OR.230 Infoturbealane välisaruandluskava

a) Organisatsioon rakendab infoturbealast aruandlussüsteemi, mis vastab määruses (EL) nr 376/2014 ning selle delegeeritud õigusaktides ja rakendusaktides sätestatud nõuetele, kui kõnealust määrust organisatsiooni suhtes kohaldatakse.

b) Ilma et see piiraks määruses (EL) nr 376/2014 sätestatud kohustusi, tagab organisatsioon, et ta teavitab oma pädevat asutust kõigist infoturvaintsidentidest või turvaaukudest, mis võivad kujutada endast märkimisväärset riski lennuohutusele. Lisaks kohaldatakse järgmist:

1) kui selline intsident või turvaauk mõjutab õhusõidukit või sellega seotud süsteemi või komponenti, teatab organisatsioon sellest ka projekti kinnituse omanikule;

2) kui selline intsident või turvaauk mõjutab organisatsioonis kasutatavat süsteemi või komponenti, teatab organisatsioon sellest süsteemi või komponendi konstrueerimise eest vastutavale organisatsioonile.

c) Organisatsioon edastab alapunktis b osutatud olukordade kohta teavet järgmiselt:

1) pädevat asutust ja vajaduse korral projekti kinnituse omanikku või süsteemi või komponendi projekteerimise eest vastutavat organisatsiooni teavitatakse kohe, kui organisatsioon asjaomasest olukorrast teada saab;

2) pädevat asutust ja vajaduse korral projekti kinnituse omanikku või süsteemi või komponendi projekteerimise eest vastutavat organisatsiooni teavitatakse nii kiiresti kui võimalik, kuid mitte hiljem kui 72 tundi pärast seda, kui organisatsioon asjaomasest olukorrast teada saab, välja arvatud erakorraliste takistavate asjaolude korral.

Teade koostatakse pädeva asutuse määratud vormis ja see peab sisaldama kogu asjakohast teavet, mida organisatsioon on olukorra kohta kogunud;

3) pädevale asutusele ja vajaduse korral projekti kinnituse omanikule või süsteemi või komponendi projekteerimise eest vastutavale organisatsioonile esitatakse järelaruanne, milles on üksikasjalikult kirjeldatud meetmeid, mida organisatsioon on intsidendist taastumiseks võtnud või kavatseb võtta, ning meetmeid, mida ta kavatseb võtta samasuguste infoturvaintsidentide vältimiseks tulevikus.

Järelaruanne esitatakse kohe, kui need meetmed on kindlaks määratud, ja see koostatakse pädeva asutuse määratud vormis.

IS.D.OR.235 Allhankelepingu sõlmimine infoturbe haldamiseks

a) Kui organisatsioon sõlmib punktis IS.D.OR.200 osutatud tegevuse mis tahes osa teostamiseks allhankelepingu mõne muu organisatsiooniga, peab ta tagama, et lepinguga hõlmatud tegevus vastab käesoleva määruse nõuetele ja et lepingupartner töötab tema järelevalve all. Organisatsioon tagab, et allhanketegevusega seotud riske juhitakse nõuetekohaselt.

b) Organisatsioon tagab, et pädeval asutusel on taotluse korral juurdepääs allhankelepingu alusel tegutsevale organisatsioonile, et teha kindlaks käesolevas määruses sätestatud kohaldatavate nõuete jätkuv järgimine.

IS.D.OR.240 Töötajatele esitatavad nõuded

a) Organisatsiooni vastutav juhataja või projekteerimisorganisatsiooni puhul selle juht, kes on määratud määruse (EL) nr 748/2012 ja määruse (EL) nr 139/2014 kohaselt, nagu on osutatud käesoleva määruse artikli 2 punkti 1 alapunktides a ja b, vastutab organisatsiooni esindajana selle eest, et organisatsioonis on kõiki käesoleva määrusega nõutavaid toiminguid võimalik rahastada ja ellu viia. See isik peab tegema järgmist:

1) tagama, et käesoleva määruse nõuete täitmiseks on olemas kõik vajalikud vahendid;

2) kehtestama punkti IS.D.OR.200 alapunkti a alapunktis 1 osutatud infoturvapoliitika ja seda edendama;

3) tõendama, et tal on olemas põhiteadmised käesoleva määruse kohta.

b) Vastutav juhataja või projekteerimisorganisatsiooni puhul selle juht määrab isiku või isikute rühma, et tagada organisatsiooni vastavus käesoleva määruse nõuetele, ning määrab kindlaks oma volituste ulatuse. Kõnealune isik või isikute rühm allub otse vastutavale juhatajale või projekteerimisorganisatsiooni puhul selle juhile ning tal peavad olema oma kohustuste täitmiseks vajalikud teadmised, taust ja kogemused. Menetlustes tuleb kindlaks määrata, kes asendab konkreetset isikut tema pikemal äraolekul.

c) Vastutav juhataja või projekteerimisorganisatsiooni puhul selle juht määrab isiku või isikute rühma, kes vastutab punkti IS.D.OR.200 alapunkti a alapunktis 12 osutatud vastavuskontrolli eest.

d) Kui organisatsioon kasutab organisatsioonilisi infoturbestruktuure, -põhimõtteid, -protsesse ja -menetlusi koos teiste organisatsioonidega või oma organisatsiooni selliste valdkondadega, mille puhul kinnitust või deklaratsiooni ei nõuta, võib vastutav juhataja või projekteerimisorganisatsiooni puhul selle juht delegeerida oma ülesanded ühisele vastutavale isikule.

Sel juhul lepivad organisatsiooni vastutav juhataja või projekteerimisorganisatsiooni puhul selle juht ja ühine vastutav isik kokku koordineerimismeetmed, et tagada infoturbehalduse nõuetekohane integreerimine organisatsiooni.

e) Vastutav juhatajavõi projekteerimisorganisatsiooni juht või alapunktis d osutatud ühine vastutav isik vastutab organisatsiooni esindajana punkti IS.D.OR.200 rakendamiseks vajalike organisatsiooniliste struktuuride, põhimõtete, protsesside ja menetluste ning nende haldamise eest organisatsioonis.

f) Organisatsioonis kehtestatakse kord, millega tagatakse, et käesoleva lisaga hõlmatud toiminguteks on piisaval arvul töötajaid.

g) Organisatsioonis kehtestatakse kord, millega tagatakse, et alapunktis f osutatud töötajatel on oma ülesannete täitmiseks vajalik pädevus.

h) Organisatsioonis kehtestatakse kord, millega tagatakse, et töötajad on teadlikud neile määratud rollide ja ülesannetega seotud kohustustest.

i) Organisatsioon peab tagama, et selliste töötajate identiteedi ja usaldusväärsuse nõuetekohase kontrolli, kellel on juurdepääs infosüsteemidele ja andmetele, mille suhtes kohaldatakse käesoleva määruse nõudeid.

IS.D.OR.245 Andmete säilitamine

a) Organisatsioon registreerib oma infoturbehaldustoimingud.

1) Organisatsioon tagab järgmiste dokumentide arhiveerimise ja jälgitavuse:

i) kõik punkti IS.D.OR.200 alapunkti e kohaselt saadud load ja nendega seotud turvariskihindamised;

ii) punkti IS.D.OR.200 alapunkti a alapunktis 9 osutatud allhankelepingud;

iii) teave punkti IS.D.OR.200 alapunktis d osutatud peamiste protsesside kohta;

iv) teave punktis IS.D.OR.205 osutatud riskihindamise käigus kindlaks tehtud riskide kohta koos punktis IS.D. OR.210 osutatud asjakohaste riskikäsitlusmeetmetega;

v) andmed punktides IS.D.OR.215 ja IS.D.OR.230 osutatud aruandluskavade kohaselt teatatud infoturvaintsidentide ja turvaaukude kohta;

vi) teave selliste infoturvasündmuste kohta, mida võib avastamata infoturvaintsidentide või turvaaukude kindlakstegemiseks olla vaja uuesti hinnata.

2) Alapunkti 1 alapunktis i osutatud teavet säilitatakse vähemalt viis aastat pärast asjaomase loa kehtivuse lõppemist.

3) Alapunkti 1 alapunktis ii osutatud teavet säilitatakse vähemalt viis aastat pärast allhankelepingu muutmist või lõpetamist.

4) Alapunkti 1 alapunktides iii, iv ja v osutatud teavet säilitatakse vähemalt viis aastat.

5) Alapunkti 1 alapunktis vi osutatud teavet säilitatakse seni, kuni asjaomased infoturvasündmused on organisatsiooni kehtestatud perioodilisusega ümber hinnatud.

b) Organisatsioon registreerib infoturbehaldustöötajate kvalifikatsiooni ja kogemused.

1) Töötajate kvalifikatsiooni ja kogemusi käsitlevat teavet säilitatakse seni, kuni isik töötab organisatsiooni heaks, ja vähemalt kolm aastat pärast seda, kui asjaomane isik on organisatsioonist lahkunud.

2) Töötajate taotlusel tagatakse neile juurdepääs oma isiklikele dokumentidele. Lisaks esitab organisatsioon lahkuvatele töötajatele nende taotlusel koopia isiklikest dokumentidest.

c) Dokumentide vorming sätestatakse organisatsiooni tegevuskorras.

d) Dokumente säilitatakse nii, et need oleks kaitstud rikkumise, muutmise ja varguse eest, ning vajaduse korral määratakse kindlaks teabe salastatusaste. Organisatsioon kasutab asjakohaseid vahendeid dokumentide tervikluse ja autentsuse säilitamiseks ning tagab, et neile pääsevad juurde ainult lubatud isikud.

IS.D.OR.250 Infoturbehalduse käsiraamat

a) Organisatsioon teeb pädevale asutusele kättesaadavaks infoturbehalduse käsiraamatu ning vajaduse korral kõik selles viidatud käsiraamatud ja menetlused, mis sisaldavad järgmist teavet:

1) vastutava juhataja või projekteerimisorganisatsiooni puhul selle juhi allkirjastatud dokument, milles kinnitatakse, et organisatsioon tegutseb pidevas kooskõlas käesoleva lisaga ja infoturbehalduse käsiraamatuga. Kui vastutav juhataja või projekteerimisorganisatsiooni puhul selle juht ei ole organisatsiooni tegevjuht, peab kinnituse allkirjastama ka organisatsiooni tegevjuht;

2) punkti IS.D.OR.240 alapunktides b ja c osutatud isiku(te) ametinimetus(ed), nimi (nimed), kohustused, vastutus, ülesanded ja volitused;

3) vajaduse korral punkti IS.D.OR.240 alapunktis d osutatud isiku(te) ametinimetus(ed), nimi (nimed), kohustused, vastutus, ülesanded ja volitused;

4) organisatsiooni infoturvapoliitika, millele on osutatud punkti IS.D.OR.200 alapunkti a alapunktis 1;

5) töötajate arvu ja kategooriate ning töötajate olemasolu planeerimiseks kasutatava süsteemi üldine kirjeldus vastavalt punkti IS.D.OR.240 nõuetele;

6) punkti IS.D.OR.200 rakendamise eest vastutavate võtmeisikute, sealhulgas punkti IS.D.OR.200 alapunkti a alapunktis 12 osutatud vastavuskontrolli funktsiooni eest vastutava(te) isiku(te) ametinimetus(ed), kohustused, vastutus, ülesanded ja volitused;

7) organisatsiooni skeem, milles on näidatud alapunktides 2 ja 6 osutatud isikute aruandlus- ja vastutusahelad;

8) punktis IS.D.OR.215 osutatud sisearuandluskava kirjeldus;

9) menetlused, milles täpsustatakse, kuidas organisatsioon tagab käesoleva osa nõuete täitmise, ning eelkõige:

i) punkti IS.D.OR.200 alapunktis c osutatud dokumenteerimistoimingud;

ii) menetlused, millega määratakse kindlaks, kuidas organisatsioon kontrollib punkti IS.D.OR.200 alapunkti a alapunktis 9 osutatud lepingulist tegevust;

iii) alapunkti c kohane menetlus infoturbehalduse käsiraamatu muutmiseks;

10) loetelu nõuete täitmise alternatiivsetest meetoditest, mis on praegu heaks kiidetud.

b) Infoturbehalduse käsiraamatu esimene väljaanne kiidetakse heaks ja pädev asutus säilitab selle koopia. Infoturbehalduse käsiraamatut muudetakse vastavalt vajadusele, et tagada organisatsiooni infoturbe halduse süsteemi kirjelduse ajakohasus. Pädevale asutusele esitatakse koopia kõigist infoturbehalduse käsiraamatu muudatustest.

c) Infoturbehalduse käsiraamatu muudatusi hallatakse organisatsiooni kehtestatud korras. Pädev asutus peab heaks kiitma kõik muudatused, mille suhtes asjaomast korda ei kohaldata, ja muudatused, mis on seotud punkti IS.D.OR.255 alapunktis b osutatud muudatustega.

d) Organisatsioon võib infoturbehalduse käsiraamatu integreerida muude olemasolevate juhtkonna näidismaterjalide või käsiraamatutega, kui on olemas selged ristviited, mis näitavad, millised juhtkonna näidismaterjali või käsiraamatu osad vastavad käesolevas lisas esitatud eri nõuetele.

IS.D.OR.255 Infoturbe halduse süsteemi muudatused

a) Infoturbe halduse süsteemi muudatusi võib hallata ja neist võib pädevat asutust teavitada organisatsiooni väljatöötatud korras. Selle korra peab heaks kiitma pädev asutus.

b) Kui asjaomase infoturbe halduse süsteemi muudatuste suhtes ei kohaldata alapunktis a osutatud korda, peab organisatsioon esitama need pädevale asutusele heakskiidu taotlemiseks ning selle saamiseks.

Kõnealuste muudatuste suhtes kohaldatakse järgmist:

1) taotlus tuleb esitada enne muudatuse tegemist, et pädeval asutusel oleks võimalik kontrollida, kas organisatsioon vastab jätkuvalt käesolevas määruses sätestatud nõuetele, ning vajaduse korral muuta organisatsiooni sertifikaati ja sellele lisatud sertifitseerimistingimusi;

2) organisatsioon teeb pädevale asutusele kättesaadavaks kogu teabe, mida nõutakse muudatuse hindamiseks;

3) muudatust rakendatakse alles siis, kui pädevalt asutuselt on selle kohta saadud ametlik heakskiit;

4) organisatsioon peab selliste muudatuste rakendamise ajal tegutsema pädeva asutuse ettenähtud tingimustel.

IS.D.OR.260 Pidev täiustamine

a) Organisatsioon hindab asjakohaste tulemusnäitajate abil infoturbe halduse süsteemi tulemuslikkust ja küpsust. Hindamine toimub organisatsiooni poolt eelnevalt kindlaks määratud ajakava alusel või pärast infoturvaintsidenti.

b) Kui alapunkti a kohase hindamise käigus leitakse puudusi, võtab organisatsioon vajalikud parandusmeetmed selle tagamiseks, et infoturbe halduse süsteem vastaks jätkuvalt kohaldatavatele nõuetele ja et infoturvariskide tase oleks jätkuvalt vastuvõetav. Lisaks hindab organisatsioon uuesti infoturbe halduse süsteemi neid elemente, mida vastuvõetud meetmed mõjutavad.